Dati Anagrafici

Nome	
Luogo e data di nascita	
Nazionalità	Italiana

Profilo Professionale

laureato in Ingegneria delle Telecomunicazioni presso l'Università la Sapienza di Roma.

Entra a far parte dell'Istituto Poligrafico e Zecca dello Stato nel 2015, dove attualmente è il Chief Security Officer (CSO), ricoprendo la posizione di Responsabile della struttura di Security & Cyber Defence, struttura all'interno della quale vengono svolte le attività legate sia alla Cyber Security che alla Physical Security.

Ha maturato un significativo background in ambito security, nel corso della sua carriera lavorando in contesti nazionali ed internazionali lavorando per diverse realtà pubbliche e private presso alcune delle maggiori società di consulenza, tra cui EY e NTTDATA, specializzandosi su tematiche di information Security, tra le quali Security Governance, Security Audit e Security Risk Assessment.

Frequentatore della 73-esima sessione del corso IASD (Istituto Alti Studi per la Difesa) presso il Centro Alti Studi per la Difesa, ha conseguito inoltre un Master di II Livello presso l'Università di Torino in "Sicurezza e Strategia Globale".

Esperienze Professionali

Periodo (da – a)	Da Ottobre 2015 ad Oggi
	Istituto Poligrafico e Zecca dello Stato
• Tipo di azienda o settore	Azienda Industriale – grafica ed editoriale
• Tipo di impiego	Dirigente

Principali mansioni e responsabilità

Responsabile U.O. Security & Cyber Defence (Da Luglio 2021 ad Oggi)

- Definire linee guida, obiettivi, requisiti di sicurezza e procedure in materia di sicurezza logica e sicurezza fisica, in linea con gli standard e normative di riferimento e di attuazione dei relativi sistemi di gestione, con l'obiettivo di garantire la protezione del patrimonio aziendale e anche al fine del raggiungimento di obiettivi di efficientamento e integrazione
- Assicurare le attività di prevenzione, rilevazione e di monitoraggio delle minacce sia sotto il profilo della sicurezza fisica che logica, di gestione degli incidenti di sicurezza e di relativa individuazione, indirizzo e attuazione, avvalendosi del supporto della struttura IT e delle altre funzioni aziendali, di misure correttive e di mitigazione a tutela del patrimonio e della continuità operativa aziendale
- Collaborare, avvalendosi del servizio interno CERT (POLI-CERT), con le autorità nazionali e internazionali per l'*infosharing* e la prevenzione di potenziali attacchi informatici
- Assicurare la gestione, la configurazione e la manutenzione applicativa dei relativi sistemi di analisi e correlazione degli eventi di sicurezza logica (SIEM) e fisica (PSIM)
- Assicurare le attività di controllo accessi e, in collaborazione con le competenti strutture aziendali, il servizio di sorveglianza fisica (es. accessi, servizi di vigilanza) per la tutela dei prodotti "valori", dei beni patrimoniali e dei dati del Poligrafico, nonché curare i rapporti con le forze

dell'ordine e con gli altri enti istituzionali competenti in materia
- Garantire l'aggiornamento dell'analisi dei rischi di sicurezza logica e fisica, in linea con lo sviluppo aziendale e con le normative vigenti in ambito sicurezza
- Assicurare, in coordinamento con le altre strutture a vario titolo coinvolte, l'attuazione di audit interni e di *assessment* di sicurezza *(vulnerability assessment* e *penetration test*), per la corretta implementazione delle disposizioni in materia di sicurezza
- Indirizzare, attuare e supervisionare, avvalendosi del supporto della Struttura IT e delle altre funzioni aziendali per le relative attività di competenza, le azioni necessarie per il mantenimento della conformità alle disposizioni in materia di cybersicurezza previste dalle normative vigenti applicabili
- Promuovere attività di sensibilizzazione e di formazione del personale in materia di sicurezza delle informazioni, di cybersecurity e di sicurezza fisica
- Definire e monitorare il piano strategico della sicurezza, in coerenza con il Piano Industriale aziendale, e assicurare la predisposizione del Budget annuale nonché il relativo Piano dei Fabbisogni
- Inoltre, sono affidati i seguenti ruoli:
- **Punto di Contatto ai sensi del D.lgs. 138/2024 (NIS2)**, al fine di coordinare e supervisionare, in collaborazione con le altre strutture a vario titolo coinvolte, l'attuazione delle disposizioni del decreto NIS, relazionando periodicamente agli organi di amministrazione, nonché interloquire con l'Autorità nazionale competente NIS.
- **Incaricato della gestione dell'attuazione delle disposizioni del decreto-legge 21 settembre 2019, n. 105, nonché della gestione delle informazioni**, al fine di coordinare e supervisionare, in collaborazione con le altre strutture a vario titolo coinvolte, l'attuazione delle disposizioni previste, nonché interloquire con l'Agenzia per la Cybersicurezza Nazionale e le altre Autorità nazionali

Principali mansioni e responsabilità

Responsabile U.O. Cyber Security (Da Settembre 2017 a Giugno 2021)
Responsabile Risk Management
- Definire strategie, obiettivi, policy, linee guida e procedure in materia di sicurezza delle informazioni in linea con gli standard di riferimento e delle normative di sicurezza informatica (stardard ISO, Misure minime Agid, protezione dati personali/privacy, ecc.), nonché attivare le iniziative necessarie al raggiungimento degli obiettivi definiti
- Gestire, quale strumento di azione preventiva, le attività di pianificazione e rivelazione delle minacce volte all'individuazione e mitigazione delle possibili vulnerabilità presenti nelle infrastrutture e nei sistemi informativi dedicati alla produzione dei servizi erogati, anche attraverso la gestione dei contratti con gli stakeholders rilevanti per la sicurezza informatica (CSIRT appartenenti alle altre istituzioni, nazionali e internazionali, CNAIPIC ecc.)
- Garantire, con il coordinamento della struttura di risk management, l'aggiornamento dell'analisi dei rischi di sicurezza delle informazioni in linea con l'evoluzione del business e con le normative cogenti in ambito sicurezza
- Assicurare, attraverso audit interni, vulnerability assessment e penetration test in coordinamento con la direzione internal auditing e le altre strutture aziendali, la corretta implementazione delle disposizioni in materia di sicurezza delle informazioni, nonché individuare le soluzioni operative e tecniche per la prevenzione, rivelazione e reazione nei riguardi degli incidenti informatici
- Definire i requisiti di sicurezza della rete e dei device (dispositivi), inclusi i

	controlli necessari per proteggere il software e le applicazioni in conformità con i requisiti di sicurezza (sistemi operativi, applicazioni, sistemi di gestione di database, applicazioni web, COTS) - Monitorare le minacce di sicurezza logica e sicurezza fisica ed eseguire analisi degli eventi durante il processo di gestione degli incidenti, definendo e indirizzando le azioni necessarie per l'avvio di azioni correttive riguardanti violazioni della sicurezza
Ruolo Aziendale	Responsabile IT Audit (Da Settembre 2016 a Settembre 2017)
Principali mansioni e responsabilità	Progetto: Governance Security Assessment. Framework di riferimento: ISO/IEC 27001:2013; Cyber Security Framework Nazionale; Misure minime di sicurezza per la Pubblica Amministrazione. Vulnerability Assessment & Penetration Test infrastrutturale interno, esterno e Web application assessment su applicazioni critiche.
Ruolo Aziendale	IT Security & Compliance Manager (Da Ottobre 2015 ad Agosto 2016)
Principali mansioni e responsabilità	Progetto: Business Impact Analysis e redazione dello Studio di Fattibilità Tecnica per la continuità operativa secondo quanto previsto dall'Art. 50 bis del CAD e dalle linee guida per il Disaster Recovery delle Pubbliche Amministrazioni AgiD.
Periodo (da – a)	Da Aprile 2015 ad Ottobre 2015
	Prometeo Management Consulting
Tipo di azienda o settore	IT Security Governance Risk & Compliance
Principali mansioni e responsabilità	Responsabile di progetti su tematiche di IT Security Governance per primarie società italiane nel settore Oil & Gas e nel settore Bancario
Periodo (da – a)	Da Gennaio 2008 ad Marzo 2015
	Ernst & Young
Tipo di azienda o settore	Information Technology Risk & Assurance
	Responsabile della gestione ed esecuzione dei seguenti progetti:
Settembre 2014 – Febbraio 2015	Business Impact Analysis e predisposizione del sistema documentale previsto dallo standard ISO22301 per il Business Continuity Management System per primaria società in ambito postale, bancario e assicurativo.
Maggio 2014 – Dicembre 2014	Disegno del processo di IT Security Risk Management, secondo quanto previsto dallo standard ISO 27001/ ISO 31000 per primaria società in ambito postale, bancario e assicurativo.
Settembre 2012 – Luglio 2014	Attività di IT security audit per la revisione del bilancio di una primaria società multinazionale nel settore Energy. Analisi e valutazione del sistema di controllo interno IT. Analisi approfondita dell'IT Enviroment del gruppo e dei processi di IT Governance per la gestione dei sistemi informativi in scope. Analisi e verifica dei processi di migrazione di sistemi afferenti a società estere del gruppo. Analisi della Segregation of duties dei sistemi ERP.
Luglio 2012 – Marzo 2015	Attività di IT security audit per la revisione del bilancio di una società multinazionale nel settore dell'intrattenimento digitale, nelle telecomunicazioni e nei servizi a valore aggiunto (Roma e New York City).
Febbraio 2012 – Gennaio 2014	Attività di Assessment e Monitoraggio del processo di Revenue Assurance di una primaria società nel settore del Gaming.
Luglio 2011 – Marzo 2014	Attività di IT security audit (SOX Compliance) per la revisione del bilancio di una delle principali società di telecomunicazioni nazionale.
Ottobre 2012 – Aprile 2013	Business Impact Analysis e Review del Disaster Recovery per primaria società in ambito servizi e infrastrutture. Individuazione dei processi critici, definizione dei parametri di ripristino RTO e RPO, esecuzione di una GAP Analysis e di

	un'analisi di fattibilità e costi/benefici, per l'implementazione di un nuovo sito di DR.
Maggio 2011 - Luglio 2011	Definizione di una Gap Analysis rispetto allo standard ISO 22301 per un ente pubblico italiano. Individuazione dei Gap documentali e Tecnologici per una corretta gestione della Business Continuity.
Marzo 2011	Assessment di sicurezza relativamente al Provvedimento del garante privacy del 27 novembre 2008 sugli amministratori di sistema per primaria società nel settore Oil & Gas.
Giugno 2010 – Ottobre 2010	Business Impact Analysis e Review del Disaster Recovery per un ente pubblico italiano. Individuazione dei processi critici, definizione dei parametri di ripristino RTO e RPO.
Aprile 2010 – Giugno 2010	Analisi e la valutazione dei rischi sui processi aziendali di Enterprise Risk Management (ERM) per primaria società in ambito postale, bancario e assicurativo. Definizione approccio metodologico per l'analisi dei rischi operativi sui processi aziendali.
Marzo 2010	Risk Assessment relativo alla compliance alla legge 231 per i reati informatici per primaria società nel settore Oil & Gas.
Dicembre 2009 – Giugno 2010	Definizione delle logiche di predisposizione del Piano Strategico della sicurezza e costruzione del cruscotto di monitoraggio della sicurezza logica per una multinazionale nel settore Energy.
Settembre 2009 – Dicembre 2009	Definizione dei requisiti funzionali per attività in ambito compliance 262/05 riguardo Log&Incident Management Applicativo/Infrastrutturale, Configuration Management, SAP Solution Manager per primaria società internazionale nel settore della difesa, dell'aerospazio e della sicurezza.
Settembre 2008 settembre 2009	Attività di IT Security Audit per la compliance alla legge 262/05 per primaria società internazionale nel settore della difesa, dell'aerospazio e della sicurezza. Analisi dell'area IT in termini di IT General Control (Entity level, Application level, Infrastructure level) nell'ambito dei processi ritenuti critici e di particolare interesse ai fini della compliance 262 per 11 società del gruppo.
Gennaio 2008 – Settembre 2008	Attività di IT Security Audit ai fini della revisione del bilancio per aziende industriali e società di servizi.

Periodo (da – a)	2005 – Gennaio 2008
Nome e indirizzo datore di lavoro	Value Partners Group: Value Team S.P.A
Tipo di azienda o settore	Consulenza direzionale e soluzioni di Information Technology
Marzo 2007 – Gennaio 2008	Attività di Program Management per la gestione e supervisione del processo di Revenue Assurance Mobile di una delle principali società di telecomunicazioni nazionale.
Settembre 2006 – Marzo 2007	Evoluzione del sistema di Service Quality Management per i servizi VAS erogati da una delle principali società di telecomunicazioni nazionale. Traduzione dei requisiti in specifiche funzionali per l'istallazione dei modelli di servizio sulla piattaforma dedicata al monitoraggio della Qualità del Servizio, dei servizi mobili e fissi (KPI e KQI). Supporto alla fase di Test e collaudo (Prove di verifica e validazione – PVV/ Prove di qualità in rete - PQR).
2005- 2006	Supporto nel disegno di dettaglio e nella implementazione delle strategie di contact CRM (Customer Relationship Management) per una primaria società nel settore del trasporto ferroviario.

Istruzione e Formazione

Periodo (da – a)	2021 –2022
Nome e tipo di istituto di istruzione o formazione	Centro Alti Studi per la Difesa 73° Sessione del Corso Istituto Alti Studi per la Difesa
Livello nella classificazione nazionale	110/110 e Lode

Periodo (da – a)	2021 –2022
Nome e tipo di istituto di istruzione o formazione	Università degli Studi di Torino Master II Livello – CMU2 in "Strategia Globale e Sicurezza"
Livello nella classificazione nazionale	110/110 e Lode

Periodo (da – a)	1998 –2005
Nome e tipo di istituto di istruzione o formazione	Università degli Studi di Roma La Sapienza Laurea Specialistica in Ingegneria delle Telecomunicazioni
Livello nella classificazione nazionale	110/110 e Lode
Lavoro di tesi	Titolo Tesi: *"Realizzazione di un sistema di protezione automatico software/hardware in reti ottiche Gigabit Ethernet".* Tesi svolta presso i laboratori dell'Istituto Superiore delle Comunicazioni (ISCOM). Il testbed, grazie alla qualità dei risultati ottenuti, è stato mostrato nell'area demo della *conferenza NGI il 18.4.2005* presso il Ministero delle Comunicazioni.

Periodo (da – a)	1992 – 1997
Nome e tipo di istituto di istruzione o formazione	Istituto Tecnico Industriale E.Fermi di Roma
Livello nella classificazione nazionale	60/60

Pubblicazioni e Conferenze	- F. Matera, A.Tarantino, F. Cugini et alt., *"Experimenting with Commercial Router MPLS Recovery Schemes"* BBEurope 2005, Bordeaux, Francia. - F. Matera, A.Tarantino, V.Baroncini et alt, "*Comparison between objective and subjective measurements of Qualità of Service over an integrated Wide Area network"* Fiber and Integrated Optics, accettato il 17 Novembre 2005. - A.Tarantino, F. Matera, L. Rea et alt., *"e-Photon/One Demonstrator at NGI conference"* e-Photon One NewsLetter, Aprile 2005. - A.Tarantino, L. Rea "QoS in an optical integrated Network: DiffServ over MPLS, objective and subjective measurements" NGI 2005, Roma Ministero delle Comunicazioni, Poster per la presentazione.
Corsi di Formazione	- Corso per certificazione di Associate Business Continuity Professional presso il Disaster Recovery Institute Italy - Corso per certificazione BS25999 Business Continuity Management Systems Auditor/Lead Auditor - Corso per certificazione ISO22301 Business Continuity Management - Corso CISA (Certified Information System Auditor) - Corso TSRS SAP R/3 Foundation Learning CEWA presso la sede di Ernst &

Young Buxelles
- Corso sulla configurazione di Router Juniper della serie M presso il Ministero delle Comunicazioni.
- Corso di Time Management e Basic Communication skills

Capacità e competenze personali

Madrelingua	Italiano
Altre lingue	Inglese
Capacità di lettura	Buono
Capacità di scrittura	Buono
Capacità di espressione orale	Buono